(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월04일
(11) 등록번호 10-2186114
(24) 등록일자 2020년11월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 9/54* (2018.01)
H04L 29/06 (2006.01) *H04L 9/14* (2006.01)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
H04W 12/06 (2009.01) *H04W 12/08* (2009.01)
H04W 12/12 (2009.01)
(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 63/061 (2013.01)
(21) 출원번호 10-2018-7030030
(22) 출원일자(국제) 2017년03월24일
심사청구일자 2020년03월17일
(85) 번역문제출일자 2018년10월17일
(65) 공개번호 10-2019-0018612
(43) 공개일자 2019년02월25일
(86) 국제출원번호 PCT/US2017/024084
(87) 국제공개번호 WO 2017/165807
국제공개일자 2017년09월28일
(30) 우선권주장
15/081,447 2016년03월25일 미국(US)
(56) 선행기술조사문헌
US20030065941 A1
US20060200660 A1
WO2015133482 A1
EP2355401 A1

(73) 특허권자
팜, 티엔, 반
미국 워싱턴 98513, 레이시, 코트 사우스이스트 24번가 9227
(72) 발명자
팜, 티엔, 반
미국 워싱턴 98513, 레이시, 코트 사우스이스트 24번가 9227
(74) 대리인
김태홍, 김진희

전체 청구항 수 : 총 21 항 심사관 : 양종필

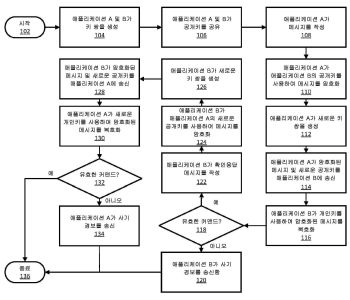
(54) 발명의 명칭 **암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 방법, 시스템, 및 매체**

(57) 요 약

암호화된 메시지를 전송하기 위한 방법, 시스템, 및 매체가 제공된다. 몇몇 구성에서, 방법은 제1 애플리케이션에 의해 하드웨어 프로세스를 사용하여, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것; 제1 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션으로부터 제2 공개키를 수신하는 것; 제2 애플

(뒷면에 계속)

대 표 도



리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것; 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하는 것; 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하는 것; 및 제2 개인키를 사용하여 제2 메시지를 복호화하는 것을 포함한다.

(52) CPC특허분류
H04L 63/101 (2013.01)
H04L 63/1441 (2013.01)
H04L 9/0861 (2013.01)
H04L 9/0891 (2013.01)
H04L 9/14 (2013.01)
H04L 9/30 (2013.01)
H04L 9/32 (2013.01)
H04W 12/06 (2019.01)
H04W 12/08 (2019.01)

명 세 서

청구범위

청구항 1

암호화된 메시지를 전송하기 위한 방법으로서,

제1 애플리케이션에 의해 하드웨어 프로세스를 사용하여, 상기 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 단계;

상기 제1 공개키를 제2 애플리케이션에 전송하는 단계;

상기 제2 애플리케이션으로부터 제2 공개키를 수신하는 단계;

암호화된 메시지를 형성하기 위하여 상기 제2 애플리케이션에 대응하는 상기 제2 공개키를 사용하여 제1 메시지를 암호화하는 단계;

상기 제1 애플리케이션에 의해, 상기 암호화된 메시지가 곧 전송되려고 하는 것에 응답하여, 제3 공개키 및 제3 개인키를 생성하는 단계;

상기 암호화된 메시지 및 상기 제3 공개키를 상기 제2 애플리케이션에 전송하는 단계;

상기 제2 애플리케이션으로부터, 상기 제2 애플리케이션에 대응하는 제2 메시지 - 상기 제2 메시지는 상기 제3 공개키를 사용하여 암호화된 것임 - 및 제4 공개키를 수신하는 단계; 및

상기 제3 개인키를 사용하여 상기 제2 메시지를 복호화하는 단계

를 포함하는 암호화된 메시지를 전송하기 위한 방법.

청구항 2

제1항에 있어서, 상기 제1 메시지는 상기 제2 애플리케이션과 연계된 인터넷 프로토콜(Internet Protocol: IP) 어드레스를 포함하는 것인 방법.

청구항 3

제1항에 있어서,

상기 제2 메시지 내에 포함된 커맨드(command)가 유효한 커맨드인지 여부를 결정하는 단계; 및

상기 커맨드가 유효한 커맨드가 아니라는 결정에 응답하여, 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 단계

를 더 포함하는 방법.

청구항 4

제3항에 있어서, 상기 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 단계는, 상기 적어도 하나의 사용자 디바이스에 문자 메시지 및 상기 적어도 하나의 사용자 디바이스와 연계된 사용자 계정에 이메일 중 적어도 하나를 전송하는 단계를 포함하는 것인 방법.

청구항 5

제3항에 있어서, 상기 커맨드가 유효한 커맨드인지 여부를 결정하는 단계는, 상기 커맨드가 상기 제1 애플리케이션에 알려져 있는지 여부를 결정하는 단계를 포함하는 것인 방법.

청구항 6

제1항에 있어서, 상기 제1 메시지의 콘텐츠는 2진 데이터 및 텍스트 데이터 중 적어도 하나를 포함하는 것인 방법.

청구항 7

제1항에 있어서, 상기 제2 메시지는 상기 제2 애플리케이션으로부터의 확인응답 메시지인 것인 방법.

청구항 8

암호화된 메시지를 전송하기 위한 시스템으로서,

하드웨어 프로세서

를 포함하고, 상기 하드웨어 프로세서는,

제1 애플리케이션에 의해, 상기 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하고;

상기 제1 공개키를 제2 애플리케이션에 전송하고;

상기 제2 애플리케이션으로부터 제2 공개키를 수신하고;

암호화된 메시지를 형성하기 위하여 상기 제2 애플리케이션에 대응하는 상기 제2 공개키를 사용하여 제1 메시지를 암호화하고;

상기 제1 애플리케이션에 의해, 상기 암호화된 메시지가 곧 전송되려고 하는 것에 응답하여, 제3 공개키 및 제3 개인키를 생성하고;

상기 암호화된 메시지 및 상기 제3 공개키를 상기 제2 애플리케이션에 전송하고;

상기 제2 애플리케이션으로부터, 상기 제2 애플리케이션에 대응하는 제2 메시지 - 상기 제2 메시지는 상기 제3 공개키를 사용하여 암호화된 것임 - 및 제4 공개키를 수신하고;

상기 제3 개인키를 사용하여 상기 제2 메시지를 복호화하도록

프로그램되는 것인 암호화된 메시지를 전송하기 위한 시스템.

청구항 9

제8항에 있어서, 상기 제1 메시지는 상기 제2 애플리케이션과 연계된 인터넷 프로토콜(IP) 어드레스를 포함하는 것인 시스템.

청구항 10

제8항에 있어서, 상기 하드웨어 프로세서는 또한,

상기 제2 메시지 내에 포함된 커맨드가 유효한 커맨드인지 여부를 결정하고;

상기 커맨드가 유효한 커맨드가 아니라는 결정에 응답하여, 사기 경보를 적어도 하나의 사용자 디바이스에 전송하도록

프로그램되는 것인 시스템.

청구항 11

제10항에 있어서, 상기 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 것은, 상기 적어도 하나의 사용자 디바이스에 문자 메시지 및 상기 적어도 하나의 사용자 디바이스와 연계된 사용자 계정에 이메일 중 적어도 하나를 전송하는 것을 포함하는 것인 시스템.

청구항 12

제10항에 있어서, 상기 커맨드가 유효한 커맨드인지 여부를 결정하는 것은, 상기 커맨드가 상기 제1 애플리케이션에 알려져 있는지 여부를 결정하는 것을 포함하는 것인 시스템.

청구항 13

제8항에 있어서, 상기 제1 메시지의 콘텐츠는 2진 데이터 및 텍스트 데이터 중 적어도 하나를 포함하는 것인 시스템.

청구항 14

제8항에 있어서, 상기 제2 메시지는 상기 제2 애플리케이션으로부터의 확인응답 메시지인 것인 시스템.

청구항 15

프로세서에 의해 실행될 때, 상기 프로세서가 암호화된 메시지를 전송하기 위한 방법을 수행하게 하는 컴퓨터 실행 가능 명령어들을 포함하는 비일시적 컴퓨터 판독 가능 매체로서, 상기 방법은

제1 애플리케이션에 의해, 상기 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 단계;

상기 제1 공개키를 제2 애플리케이션에 전송하는 단계;

상기 제2 애플리케이션으로부터 제2 공개키를 수신하는 단계;

암호화된 메시지를 형성하기 위하여 상기 제2 애플리케이션에 대응하는 상기 제2 공개키를 사용하여 제1 메시지를 암호화하는 단계;

상기 제1 애플리케이션에 의해, 상기 암호화된 메시지가 곧 전송되려고 하는 것에 응답하여, 제3 공개키 및 제3 개인키를 생성하는 단계;

상기 암호화된 메시지 및 상기 제3 공개키를 상기 제2 애플리케이션에 전송하는 단계;

상기 제2 애플리케이션으로부터, 상기 제2 애플리케이션에 대응하는 제2 메시지 - 상기 제2 메시지는 상기 제3 공개키를 사용하여 암호화된 것임 - 및 제4 공개키를 수신하는 단계; 및

상기 제3 개인키를 사용하여 상기 제2 메시지를 복호화하는 단계

를 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 16

제15항에 있어서, 상기 제1 메시지는 상기 제2 애플리케이션과 연계된 인터넷 프로토콜(IP) 어드레스를 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 17

제15항에 있어서, 상기 방법은,

상기 제2 메시지 내에 포함된 커맨드가 유효한 커맨드인지 여부를 결정하는 단계; 및

상기 커맨드가 유효한 커맨드가 아니라는 결정에 응답하여, 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 단계

를 더 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 18

제17항에 있어서, 상기 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 단계는, 상기 적어도 하나의 사용자 디바이스에 문자 메시지 및 상기 적어도 하나의 사용자 디바이스와 연계된 사용자 계정에 이메일 중 적어도 하나를 전송하는 단계를 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 19

제17항에 있어서, 상기 커맨드가 유효한 커맨드인지 여부를 결정하는 단계는, 상기 커맨드가 상기 제1 애플리케이션에 알려져 있는지 여부를 결정하는 단계를 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 20

제15항에 있어서, 상기 제1 메시지의 콘텐츠는 2진 데이터 및 텍스트 데이터 중 적어도 하나를 포함하는 것인 비일시적 컴퓨터 판독 가능 매체.

청구항 21

제15항에 있어서, 상기 제2 메시지는 상기 제2 애플리케이션으로부터의 확인응답 메시지인 것인 비일시적 컴퓨터 판독 가능 매체.

발명의 설명

기 술 분 야

[0001] **관련 출원의 상호 참조**

[0002] 본 출원은 본 명세서에 그대로 참조로서 합체되어 있는 2016년 3월 25일 출원된 미국 특허 출원 제15/081,447호로부터 우선권을 주장한다.

[0003] **기술분야**

[0004] 개시된 요지는 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조(dynamic public key infrastructure)를 사용하기 위한 방법, 시스템, 및 매체에 관한 것이다.

배 경 기 술

[0005] 소프트웨어 애플리케이션 사이의 데이터 통신은 요구되는 만큼 보안성이 있지 않다. 다수의 소프트웨어 애플리케이션은 공유되는 단일의 키를 사용하여 대칭키 암호화에 의해 통신한다. 다른 소프트웨어 애플리케이션은 공개키 및 개인키를 사용함으로써 공개키 기반 구조(Public Key Infrastructure: PKI)를 사용하여 비대칭 암호화를 사용한다. 그러나, 이들 암호화 기술은 2개의 소프트웨어 애플리케이션 사이의 통신 링크를 보호하기에 충분하지 않다. 예를 들어, 비대칭 암호화에서, 개인키가 손상되면, 통신 링크는 보안성이 있지 않고, 통신 링크 상에서의 사람 또는 소프트웨어 스누핑(snooping)이 통신된 모든 메시지를 판독할 수 있다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0006] 암호화된 메시지를 전송하기 위한 방법, 시스템, 및 매체가 제공된다. 개시된 요지의 몇몇 구성에 따르면, 암호화된 메시지를 전송하기 위한 방법이 제공되고, 방법은 제1 애플리케이션에 의해 하드웨어 프로세스를 사용하여, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것; 제1 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션으로부터 제2 공개키를 수신하는 것; 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것; 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하는 것; 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하는 것; 및 제2 개인키를 사용하여 제2 메시지를 복호화하는 것을 포함한다.

[0007] 개시된 요지의 몇몇 구성에 따르면, 암호화된 메시지를 전송하기 위한 시스템이 제공되고, 시스템은 제1 애플리케이션에 의해 하드웨어 프로세스를 사용하여, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하고; 제1 공개키를 제2 애플리케이션에 전송하고; 제2 애플리케이션으로부터 제2 공개키를 수신하고; 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하고; 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하고; 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하고; 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하고; 제2 개인키를 사용하여 제2 메시지를 복호화하도록 프로그램된 하드웨어 프로세서를 포함한다.

[0008] 개시된 요지의 몇몇 구성에 따르면, 프로세서에 의해 실행될 때, 프로세서가 암호화된 메시지를 전송하기 위한 방법을 수행하게 하는 컴퓨터 실행 가능 명령어(instruction)를 포함하는 컴퓨터 판독 가능 매체가 제공된다. 방법은 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것; 제1 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션으로부터 제2 공개키를 수신하는 것; 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것; 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하는 것; 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이

션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하는 것; 및 제2 개인키를 사용하여 제2 메시지를 복호화하는 것을 포함한다.

[0009] 암호화된 메시지를 전송하기 위한 방법이 개시된다. 방법은 제1 애플리케이션에 의해 하드웨어 프로세스를 사용하여, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것을 포함할 수도 있다. 방법은 제1 공개키를 제2 애플리케이션에 전송하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션으로부터 제2 공개키를 수신하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것을 포함할 수도 있다. 방법은 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하는 것을 포함할 수도 있다. 방법은 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하는 것을 포함할 수도 있다. 방법은 제2 개인키를 사용하여 제2 메시지를 복호화하는 것을 포함할 수도 있다.

[0010] 방법의 단계들 중 하나 이상은 하나 이상의 프로세서에 의해 수행될 수도 있다. 하나 이상의 프로세서는 제1 및 제2 애플리케이션 중 하나 이상과 연계될 수도 있다.

[0011] 방법은 제1 및 제2 메시지 중 적어도 하나 내에 포함된 커맨드(command)가 유효한 커맨드인지 여부를 결정하는 단계를 더 포함할 수도 있다. 커맨드가 유효한 커맨드가 아니라는 결정에 응답하여, 방법은 사기 경보(fraud alert)를 적어도 하나의 사용자 디바이스에 전송하는 것을 더 포함할 수도 있다. 사기 경보를 적어도 하나의 사용자 디바이스에 전송하는 것은 적어도 하나의 사용자 디바이스에 문자 메시지 및 적어도 하나의 사용자 디바이스와 연계된 사용자 계정에 이메일 중 적어도 하나를 전송하는 것을 포함할 수도 있다. 커맨드가 유효한 커맨드가 아니라는 결정에 응답하여, 방법은 무효한 커맨드의 수신시에 애플리케이션에 의해, 커맨드가 수신되었던 애플리케이션으로부터 추가의 메시지를 차단하는 것을 더 포함할 수도 있다.

[0012] 커맨드가 유효한 커맨드인지 여부를 결정하는 것은 커맨드가 적어도 하나의 애플리케이션에 알려져 있는지 여부를 결정하는 것을 포함할 수도 있다. 커맨드는 적어도 하나의 애플리케이션과 연계된 메모리 내에 저장될 수도 있고, 커맨드가 유효한 커맨드인지 여부를 결정하는 단계는 메모리 내의 커맨드를 룩업하는 것(looking up)을 포함할 수도 있다. 커맨드는 명령어 및/또는 태그를 갖고 메모리 내에 저장될 수도 있다. 명령어 및/또는 태그는 커맨드가 유효한 커맨드인지 아닌지 여부를 지시할 수도 있다.

[0013] 제1, 제2 및 제3 키 쌍 중 적어도 하나는 제1, 제2 및 제3 키 쌍 중 적어도 다른 하나와는 상이할 수도 있다. 공개 및 개인키 쌍 중 적어도 하나는 비대칭 암호화 알고리즘을 사용하여 생성될 수도 있다.

[0014] 제1 메시지는 제2 애플리케이션과 연계된 어드레스를 포함할 수도 있다. 어드레스는 인터넷 프로토콜(Internet Protocol: IP) 어드레스일 수도 있다. 메시지의 콘텐츠는 2진 데이터 및 텍스트 데이터 중 적어도 하나를 포함할 수도 있다.

[0015] 제2 메시지는 제2 애플리케이션으로부터의 확인응답 메시지(acknowledgement message)일 수도 있다.

[0016] 암호화된 메시지를 전송하는 방법의 단계들 중 적어도 하나를 수행하도록 프로세서에 의해 실행 가능한 명령어를 포함하는 컴퓨터 판독 가능 매체가 개시된다.

[0017] 암호화된 메시지를 전송하기 위한 시스템이 개시된다. 시스템은 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하도록 프로그램된 하드웨어 프로세서를 포함할 수도 있다. 하드웨어 프로세서는 제1 공개키를 제2 애플리케이션에 전송하도록 프로그램될 수도 있다. 하드웨어 프로세서는 제2 애플리케이션으로부터 제2 공개키를 수신하도록 프로그램될 수도 있다. 하드웨어 프로세서는 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하도록 프로그램될 수도 있다. 하드웨어 프로세서는 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하도록 프로그램된다. 하드웨어 프로세서는 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하도록 프로그램될 수도 있다. 하드웨어 프로세서는 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하도록 프로그램될 수도 있다. 하드웨어 프로세서는 제2 개인키를 사용하여 제2 메시지를 복호화하도록 프로그램될 수도 있다.

[0018] 프로세서에 의해 실행될 때, 프로세서가 암호화된 메시지를 전송하기 위한 방법을 수행하게 하는 컴퓨터 실행 가능 명령어를 포함하는 컴퓨터 판독 가능 매체가 개시된다. 방법은 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것을 포함할 수도 있다. 방법은 제1 공개키를 제2 애플리케이션에 전송하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션으로부터 제2 공개키를 수신하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것을

포함할 수도 있다. 방법은 제1 애플리케이션에 의해, 제3 공개키 및 제2 개인키를 생성하는 것을 포함할 수도 있다. 방법은 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것을 포함할 수도 있다. 방법은 제2 애플리케이션으로부터, 제2 애플리케이션에 대응하는 제2 메시지 및 제4 공개키를 수신하는 것을 포함할 수도 있다. 방법은 제2 개인키를 사용하여 제2 메시지를 복호화하는 것을 포함할 수도 있다.

[0019] 암호화된 메시지를 전송하는 방법이 개시되고, 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것; 제1 애플리케이션에 의해, 제1 공개키를 제2 애플리케이션에 전송하는 것; 제2 애플리케이션에 의해, 제2 애플리케이션에 대응하는 제2 공개키 및 제2 개인키를 생성하는 것; 제1 애플리케이션에 의해, 제2 애플리케이션으로부터 제2 공개키를 수신하는 것; 제1 애플리케이션에 의해, 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하는 것; 제1 애플리케이션에 의해, 제3 공개키 및 제3 개인키를 생성하는 것; 및 제1 애플리케이션에 의해, 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것을 포함한다.

[0020] 방법은 제2 애플리케이션에 의해, 제4 공개키 및 제4 개인키를 생성하는 단계를 더 포함할 수도 있다. 방법은 제1 애플리케이션에 의해, 제2 애플리케이션으로부터 제2 메시지 및 제4 공개키를 수신하는 단계를 더 포함할 수도 있다. 방법은 제1 애플리케이션에 의해, 제2 개인키를 사용하여 제2 메시지를 복호화하는 단계를 더 포함할 수도 있다.

[0021] 암호화된 메시지를 전송하기 위한 시스템이 개시되고, 시스템은 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하고; 제1 공개키를 제2 애플리케이션에 전송하고; 제2 애플리케이션에 의해, 제2 공개키 및 제2 개인키를 생성하고; 제2 애플리케이션으로부터 제2 공개키를 수신하고; 제2 애플리케이션에 대응하는 제2 공개키를 사용하여 제1 메시지를 암호화하고; 제1 애플리케이션에 의해, 제3 공개키 및 제3 개인키를 생성하고; 암호화된 메시지 및 제3 공개키를 제2 애플리케이션에 전송하도록 프로그램된 하나 이상의 하드웨어 프로세서를 포함한다.

[0022] 제1 애플리케이션으로부터 암호화된 메시지를 전송하는 방법이 개시되고, 방법은 제1 애플리케이션에 의해, 제1 애플리케이션에 대응하는 제1 공개키 및 제1 개인키를 생성하는 것; 제1 애플리케이션에 의해, 제1 공개키를 제2 애플리케이션에 전송하는 것; 제1 애플리케이션에 의해, 제2 애플리케이션으로부터 제2 공개키를 수신하는 것으로서, 제2 공개키는 제2 애플리케이션 및 제2 개인키에 대응하는 것인, 제2 공개키를 수신하는 것; 제1 애플리케이션에 의해, 제2 공개키를 사용하여 제1 메시지를 암호화하는 것; 제1 애플리케이션에 의해, 제3 공개키 및 제3 개인키를 생성하는 것; 및 제1 애플리케이션에 의해, 제1 메시지 및 제3 공개키를 제2 애플리케이션에 전송하는 것을 포함한다.

[0023] 방법은 제1 애플리케이션에 의해, 제2 애플리케이션으로부터 제2 메시지 및 제4 공개키를 수신하는 단계를 더 포함할 수도 있고, 제2 메시지는 제3 공개키를 사용하여 암호화되고, 제3 공개키는 제2 애플리케이션에 대응한다. 방법은 제1 애플리케이션에 의해, 제3 개인키를 사용하여 제2 메시지를 복호화하는 단계를 더 포함할 수도 있다.

[0024] 제2 애플리케이션에서 암호화된 메시지를 수신하는 방법이 개시되고, 방법은 제2 애플리케이션에 의해, 제1 애플리케이션으로부터 제1 공개키를 수신하는 것으로서, 제1 공개키는 제1 애플리케이션 및 제1 개인키에 대응하는 것인, 제1 공개키를 수신하는 것; 제2 애플리케이션에 의해, 제2 애플리케이션에 대응하는 제2 공개키 및 제2 개인키를 생성하는 것; 제2 애플리케이션에 의해, 제1 애플리케이션에 제2 공개키를 전송하는 것; 제2 애플리케이션에 의해, 제1 애플리케이션으로부터 제1 메시지 및 제3 공개키를 수신하는 것으로서, 제1 메시지는 제2 공개키를 사용하여 암호화되고 제3 공개키는 제1 애플리케이션 및 제3 개인키에 대응하는 것인, 제1 메시지 및 제3 공개키를 수신하는 것을 포함한다.

[0025] 방법은 제2 애플리케이션에 의해, 제2 개인키를 사용하여 제1 메시지를 복호화하는 단계를 더 포함할 수도 있다. 방법은 제2 애플리케이션에 의해, 제4 공개키 및 제4 개인키를 생성하는 단계를 더 포함할 수도 있다. 방법은 제2 애플리케이션에 의해, 제3 개인키를 사용하여 제2 메시지를 복호화하는 단계를 더 포함할 수도 있다. 방법은 제2 애플리케이션에 의해, 제1 애플리케이션에 제2 메시지 및 제4 공개키를 전송하는 단계를 더 포함할 수도 있다.

도면의 간단한 설명

[0026] 개시된 요지의 다양한 목적, 특징, 및 장점은 유사한 도면 부호가 유사한 요소를 식별하고 있는 이하의 도면과

관련하여 고려될 때 개시된 요지의 이하의 상세한 설명을 참조하여 더 완전히 이해될 수 있다.

도 1은 개시된 요지의 몇몇 구성에 따른 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 프로세스의 예를 도시하고 있다.

도 2는 개시된 요지의 몇몇 구성에 따른 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 시스템의 예의 개략도를 도시하고 있다.

도 3은 개시된 요지의 몇몇 구성에 따른 서버 및/또는 사용자 디바이스에서 사용될 수 있는 하드웨어의 예를 도시하고 있다.

발명을 실시하기 위한 구체적인 내용

[0027] 다양한 구성에 따르면, 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 메커니즘(방법, 시스템, 및 매체를 포함할 수 있음)이 제공된다.

[0028] 특히, 소프트웨어 애플리케이션 사이의 공개키 및 개인키의 교환을 동적이 되게 하는 방법이 제공된다. 간략히, 메시지를 전송할 때마다 새로운 공개키 및 개인키가 애플리케이션에 의해 생성되어 애플리케이션의 키가 시간 경과에 따라 예측 불가능하게 변경되게 된다. 유용하게, 이는 동적으로 변경하는 공개키 개인키 쌍을 계속 따라잡아야 하기 때문에, 미권한부여된 애플리케이션이 데이터 통신 상에서 스누핑하는 것을 매우 어렵고 에너지 집약적이게 한다. 그 결과, 보안 레벨이 증가된다.

[0029] 몇몇 구성에서, 본 명세서에 설명된 메커니즘은 메시지를 암호화하고 2개의 애플리케이션(예를 들어, 모바일 디바이스 상에서 실행되는 2개의 애플리케이션, 및/또는 다른 적합한 유형의 애플리케이션) 사이에 메시지를 전송할 수 있다. 몇몇 구성에서, 메커니즘은 예를 들어, 수신된 메시지 내에 포함된 커맨드가 유효한지를 결정함으로써, 전송된 메시지를 유효화할 수 있다. 몇몇 이러한 구성에서, 메커니즘은 수신된 메시지가 무효한 것으로 결정하는 것에 응답하여 사기 경보를 전송할 수 있다. 예를 들어, 몇몇 구성에서, 사기 경보는 수신된 메시지가 무효하다는 것을 결정하는 애플리케이션에 의해 지시되어 사용자 디바이스 및/또는 사용자 계정에 전송될 수 있다. 사기 경보는 동일한 소스로부터 수신된 메시지의 주의가 되도록 이들에 경고하여 다른 소프트웨어 애플리케이션에 또한 전송될 수 있다. 유리하게는, 수신된 메시지가 무효하다는 것을 결정함으로써, 애플리케이션은 자신을 그리고/또는 애플리케이션이 실행되는 하드웨어 및 따라서 최종적으로 애플리케이션 및/또는 하드웨어의 사용자를 보호할 수 있다. 예를 들어, 애플리케이션은 데이터를 위한 요청, 암호화키를 공유하는 요청 및/또는 애플리케이션이 실행되는 하드웨어의 메모리로의 액세스를 위한 요청과 같은, 임의의 명령어를 수신된 메시지 내에서 실행하는 것을 회피할 수도 있다. 대안적으로 또는 부가적으로, 애플리케이션은 안티바이러스 및/또는 안티해킹 소프트웨어와 같은 보안 소프트웨어에 경보를 또한 전송할 수도 있다.

[0030] 몇몇 구성에서, 본 명세서에 설명된 메커니즘은 임의의 적합한 기술 또는 기술의 조합을 사용하여 메시지를 암호화 및 복호화할 수 있다. 예를 들어, 몇몇 구성에서, 제1 애플리케이션 및 제2 애플리케이션은 공개키 개인키 쌍을 각각 생성할 수 있고, 공개키를 교환할 수 있다. 제1 애플리케이션은 이어서 메시지를 생성하고 제2 애플리케이션의 공개키를 사용하여 메시지를 암호화할 수 있다. 제1 애플리케이션은 이어서 새로운 공개키 개인키 쌍을 생성할 수 있고, 새로운 공개키로 제2 애플리케이션에 메시지를 전송할 수 있다. 제2 애플리케이션은 제2 애플리케이션의 개인키를 사용하여 수신된 메시지를 복호화할 수 있다. 몇몇 구성에서, 제2 애플리케이션은 확인응답 메시지를 생성할 수 있고, 제1 애플리케이션의 공개키를 사용하여 확인응답 메시지를 암호화할 수 있다. 몇몇 구성에서, 본 명세서에 설명된 메커니즘은 모든 전송된 메시지에 대해 새로운 공개-개인키 쌍을 동적으로 생성할 수 있다. 몇몇 구성에서, 암호화 및/또는 복호화는 도 1과 관련하여 이하에 설명되는 바와 같이, 생성된 키를 사용하여 비대칭 암호화 및/또는 복호화 알고리즘을 사용하여 수행될 수 있다.

[0031] 도 1을 참조하면, 먼저 PKI 공개키 및 개인키를 생성하고, 공개키를 공유하고, 메시지를 작성하고, 메시지를 암호화하고, 새로운 PKI 공개키 및 개인키를 생성하고, 메시지 및 새로운 PKI 공개키를 송신하고, 메시지를 유효화하고, 사기 경보를 송신하고, IP 어드레스를 블랙리스팅하고, 확인응답 메시지를 송신하고, 확인응답 메시지의 진정성(authenticity)을 유효화함으로써 소프트웨어 애플리케이션 사이에 보안된 메시지를 송수신하기 위한 프로세스(100)의 예가 개시된 요지의 몇몇 구성에 따라 도시되어 있다. 이하에 더 상세히 설명되는 바와 같이, 프로세스(100)에서 언급되는 메시지는 도 2에 도시되어 있는 하드웨어에 따라 송수신될 수 있다. 또한 이하에 더 상세히 설명되는 바와 같이, 프로세스(100)는 도 3의 하드웨어(300), 또는 임의의 다른 적합한 하드웨어 구성을 사용하여 구현될 수 있다.

[0032] 프로세스(100)는 102에서 시작할 수 있다. 프로세스(100)는 이어서 블록 104로 계속될 수 있고, 여기서 애플리케이션 A 및 애플리케이션 B는 공개키 기반 구조(PKI) 공개 및 개인키 쌍을 생성할 수 있다. 애플리케이션 A 및 애플리케이션 B는 임의의 적합한 PKI 암호시스템을 사용하여 PKI 공개 및 개인키 쌍을 생성할 수 있다. PKI 암호시스템을 위한 명령어는 애플리케이션 A 및/또는 B에 로컬인 메모리(304)와 같은 메모리 내에 저장될 수도 있고, 명령어는 PKI 공개 및 개인키 쌍을 생성하도록 메모리와 통신 가능하게 커플링된 프로세서(302)와 같은 프로세서에 의해 실행 가능할 수도 있다. 예로서, 애플리케이션 A 및 애플리케이션 B는 리베스트-셰미르-아델만(Rivest-Shamir-Adleman: RSA) 암호시스템을 사용할 수 있다. 몇몇 구성에서, 애플리케이션 A 및 애플리케이션 B는 임의의 적합한 유형의 애플리케이션(예를 들어, 모바일 디바이스 상에서 실행되는 애플리케이션, 비-모바일 디바이스 상에서 실행되는 애플리케이션, 및/또는 임의의 다른 적합한 유형의 애플리케이션)일 수 있다는 것을 주목하라. 예를 들어, 애플리케이션 A 및 B는 컴퓨터 상의 애플리케이션일 수 있다. 부가적으로, 몇몇 구성에서, 애플리케이션 A 및 애플리케이션 B는 동일한 디바이스(예를 들어, 동일한 사용자 디바이스) 및/또는 상이한 디바이스 상의 애플리케이션일 수 있다.

[0033] 블록 106에서, 애플리케이션 A 및 애플리케이션 B는 공개키를 교환할 수 있다. 예를 들어, 몇몇 구성에서, 애플리케이션 A는 통신 네트워크(206)와 같은 통신 네트워크를 통해 그 PKI 공개키를 애플리케이션 B에 전송할 수 있다. 대안적으로, 애플리케이션 A 및 B가 동일한 디바이스 상의 애플리케이션인 경우에, 애플리케이션 A는 디바이스 내에서 내부적으로 그 PKI 공개키를 애플리케이션 B에 전송할 수 있다. 다른 예로서, 몇몇 구성에서, 애플리케이션 B는 그 PKI 공개키를 애플리케이션 A에 전송할 수 있다. 몇몇 구성에서, 애플리케이션 중 적어도 하나는 예를 들어 통신 네트워크(206)를 통해 그 공개키를 공공에 브로드캐스팅함으로써 그 공개키를 공공에 알려지게 할 수도 있다. 몇몇 구성에서, 일단 공개키가 애플리케이션 A와 애플리케이션 B 사이에 공유되어 있으면, 통신 링크가 애플리케이션 A와 애플리케이션 B 사이에 설정될 수 있다는 것을 주목하라. 몇몇 이러한 구성에서, 메시지는 통신 링크를 거쳐 애플리케이션 A와 애플리케이션 B 사이에 전송될 수 있다. 유리하게는, PKI의 사용에 기인하여, 통신 링크는 2개의 애플리케이션 사이의 보안 통신 링크이다.

[0034] 블록 108에서, 애플리케이션 A는 애플리케이션 B에 전송될 메시지를 생성할 수 있다. 몇몇 구성에서, 메시지는 임의의 적합한 정보를 포함할 수 있고, 임의의 적합한 포맷에 있을 수 있다. 예를 들어, 몇몇 구성에서, 메시지는 애플리케이션 B의 인터넷 프로토콜(IP) 어드레스와 같은 애플리케이션 B의 전달 어드레스; 애플리케이션 A 및 애플리케이션 B의 모두에게 알려진 커맨드; 애플리케이션 B에 전송된 메시지의 콘텐츠; 및/또는 임의의 다른 적합한 정보를 포함할 수 있다. 블록 108에서 생성된 메시지의 예시적인 포맷은: "[IP Adress]:[Command]:[Message]"일 수 있고, 여기서 "[Message]"는 메시지의 콘텐츠(예를 들어, 커맨드와 연계된 값 또는 다른 텍스트, 및/또는 임의의 다른 적합한 유형의 메시지 콘텐츠)일 수 있다. 몇몇 구성에서, 메시지의 콘텐츠는 텍스트 데이터, 2진 데이터, 및/또는 임의의 다른 적합한 포맷의 데이터일 수 있다. 상기에 제공된 예는 단지 예일 뿐이고, 몇몇 구성에서, 생성된 메시지는 임의의 적합한 포맷을 가질 수 있고, 메시지 내의 정보는 임의의 적합한 순서로 순서화될 수 있다는 것을 주목하라. 예를 들어, 몇몇 구성에서, 메시지 내의 정보는 세미콜론, 마침표, 하이픈, 및/또는 임의의 다른 적합한 구분 문자에 의해 분리될 수 있다. 이하에 더 상세히 설명되는 바와 같이, 디바이스들 사이에 메시지를 전송하기 위해 적합한 임의의 통신 네트워크가 사용될 수도 있다.

[0035] 블록 110에서, 애플리케이션 A는 블록 104에서 애플리케이션 B에 의해 생성되어 블록 106에서 애플리케이션 A에 의해 수신된 공개키를 사용하여 메시지를 암호화할 수 있다. 예를 들어, 몇몇 구성에서, 메시지는 비대칭 암호화 알고리즘을 사용하여 암호화될 수 있다.

[0036] 블록 112에서, 애플리케이션 A는 블록 104를 참조하여 설명된 것과 유사한 또는 동일한 방식으로 새로운 PKI 공개 및 개인키 쌍을 생성할 수 있다.

[0037] 블록 114에서, 애플리케이션 A는 블록 108에서 생성된 메시지 및 블록 112에서 생성된 새로운 공개키를 애플리케이션 B에 전송할 수 있다. 유리하게는, 이는 블록 114에서 메시지로 애플리케이션 A에 의해 전송된 공개키가 블록 104에서 애플리케이션 A에 의해 생성된 공개키와 이미 상이하기 때문에, 애플리케이션 A 및 애플리케이션 B가 이들 사이에 전송된 각각의 메시지로 이들의 공개키 및 개인키를 동적으로 변경하는 프로세스를 시작한다.

[0038] 블록 116에서, 애플리케이션 B는 애플리케이션 A로부터 전송된 메시지를 수신할 수 있다. 애플리케이션 B는 이어서 애플리케이션 B의 개인키를 사용하여 암호화된 메시지를 복호화할 수 있다. 몇몇 구성에서, 복호화는 비대칭 복호화 알고리즘을 사용하여 수행될 수 있다.

[0039] 블록 118에서, 애플리케이션 B는 복호화된 메시지 내에 포함된 커맨드가 유효한 커맨드인지 여부를 결정할 수

있다. 예를 들어, 몇몇 구성에서, 애플리케이션 B는 커맨드가 애플리케이션 B에 알려진 커맨드인 것을 표현하는지를 결정할 수 있다. 예를 들어, 애플리케이션 B는 커맨드가 애플리케이션 B가 실행되는 디바이스의 메모리 내에 저장된 커맨드를 표현하는지를 결정할 수 있다. 커맨드는 이러한 커맨드가 유효하고, 허용 가능하고 그리고/또는 신뢰적이라는 명령어 및/또는 태그를 갖고 애플리케이션 B가 실행되는 디바이스 메모리 내에 저장될 수도 있다. 대안적으로, 커맨드는 커맨드가 애플리케이션에 의해 실행되어서는 안되는, 무효하고, 허용 불가능하고 그리고/또는 비신뢰적인 커맨드다라는 명령어 및/또는 태그 옆에 저장될 수도 있다. 몇몇 구성에서, 애플리케이션 B는, 메시지 내에 포함된 커맨드가 유효한 커맨드다라는 결정에 응답하여, 복호화된 메시지가 인증되고 그리고/또는 손상되지 않았다고 결정할 수 있다. 몇몇 구성에서, 복호화된 메시지는 메시지가 그로부터 수신된 디바이스 또는 애플리케이션 ID 및/또는 디바이스 어드레스 - IP 어드레스와 같은 - 의 지시를 포함하고, 애플리케이션 B는 ID 및/또는 어드레스가 신뢰된 디바이스 및/또는 어드레스에 대응하는지 여부를 결정한다. 이를 행하기 위해, 애플리케이션 B는 애플리케이션 B가 실행되는 디바이스의 메모리 내의 신뢰된 애플리케이션 및/또는 디바이스에 대응하는 ID 및/또는 어드레스의 리스트 내에서 ID 및/또는 어드레스를 룩업할 수도 있다.

[0040] 블록 118에서, 애플리케이션 B가 커맨드가 유효한 커맨드다라고 결정하면(118에서 "예"), 애플리케이션 B는 블록 122에서 확인응답 메시지를 생성할 수 있다. 몇몇 구성에서, 확인응답 메시지는 임의의 적합한 정보를 포함할 수 있고, 임의의 적합한 포맷일 수 있다. 예를 들어, 몇몇 구성에서, 블록 108에서 애플리케이션 A에 의해 생성된 메시지에 유사하게, 확인응답 메시지는 애플리케이션 A의 IP 어드레스, 애플리케이션 A 및 애플리케이션 B의 모두에 알려진 커맨드, 및 임의의 적합한 메시지 콘텐츠를 포함할 수 있다. 예를 들어, 몇몇 구성에서, 메시지 콘텐츠는 블록 114에서 수신된 메시지 내의 커맨드가 성공적으로 실행되었다는 것을 지시할 수 있다. 블록 108에 유사하게, 확인응답 메시지를 위한 예시적인 포맷은: "[IP Adress]:[Command]:[Message]"이고, 여기서 "[Message]"는 메시지의 콘텐츠일 수 있고, 텍스트 데이터, 2진 데이터, 또는 임의의 다른 적합한 유형의 데이터일 수 있다. 몇몇 구성에서, 메시지 내에 포함된 정보는 임의의 적합한 순서일 수 있고, 블록 108과 관련하여 전술된 바와 같이, 임의의 적합한 유형의 구분 문자에 의해 분리될 수 있다. 몇몇 구성에서, 애플리케이션 B에 의해 생성된 확인응답 메시지의 순서 및/또는 포맷은 블록 108에서 애플리케이션 A에 의해 생성된 메시지의 순서 및/또는 포맷과 동일할 수 있다는 것을 주목하라. 대안적으로, 몇몇 구성에서, 확인응답 메시지의 순서 및/또는 포맷은 블록 108에서 애플리케이션 A에 의해 생성된 메시지의 순서 및/또는 포맷과 상이할 수 있다는 것을 주목하라.

[0041] 애플리케이션 B는 이어서 블록 124로 진행할 수 있고, 블록 112에서 애플리케이션 A에 의해 생성되어 블록 114에서 애플리케이션 B에 의해 수신된 새로운 PKI 공개키를 사용하여 확인응답 메시징을 암호화할 수 있다. 몇몇 구성에서, 애플리케이션 B는 비대칭 암호화 알고리즘을 사용하여 확인응답 메시지를 암호화할 수 있다. 애플리케이션 B는 블록 126에서 새로운 공개 및 개인키 쌍을 생성할 수 있다. 애플리케이션 B는 이어서 블록 128에서 애플리케이션 A에 암호화된 메시지 및 새로운 공개키를 전송할 수 있다. 유리하게는, 애플리케이션 B가 새로운 공개키를 생성하여 확인응답을 갖고 애플리케이션 A에 전송하기 때문에, 공개키 및 개인키를 동적으로 변경하는 프로세스는 2개의 애플리케이션 사이의 통신 링크의 보안을 더 양호하게 유지하기 위해 계속된다.

[0042] 블록 118로 복귀하면, 애플리케이션 B가 애플리케이션 A로부터 수신된 커맨드가 무효하다고 결정하면(118에서 "아니오"), 애플리케이션 B는 블록 120에서 하나 이상의 사기 경보를 송신할 수 있다. 예를 들어, 몇몇 구성에서, 애플리케이션 B는 애플리케이션 B에 의해 지시된(예를 들어, 애플리케이션 B의 제작자에 의해 지정된, 애플리케이션 B와 연계된 리스트 또는 데이터베이스 내에 저장된, 그리고/또는 임의의 다른 적합한 방식으로 애플리케이션 B에 의해 지시된) 휴대폰에 그리고/또는 애플리케이션 B에 의해 지시된(예를 들어, 애플리케이션 B의 제작자에 의해 지정된, 애플리케이션 B와 연계된 리스트 또는 데이터베이스 내에 저장된, 그리고/또는 임의의 다른 적합한 방식으로 애플리케이션 B에 의해 지시된) 이메일 어드레스에 사기 경보를 전송할 수 있다. 이 방식으로, 애플리케이션 B는 보안의 침해가 있다는 것을 사용자에게 경고할 수 있다. 애플리케이션 B는 부가적으로 또는 대안적으로 애플리케이션 A로부터 수신된 커맨드가 전술된 임의의 수의 방식으로 무효하다는 결정에 응답할 수 있다. 사기 경보가 애플리케이션 B에 의해 지시된 이메일 어드레스에 전송된 이메일인 경우에, 이메일 어드레스는 애플리케이션 B의 사용자를 위한 사용자 계정에 대응할 수 있다. 몇몇 구성에서, 사기 경보는 모바일 디바이스에 송신된 문자 메시지, 모바일 디바이스 상에 제시된 푸시 알림, 식별된 이메일 어드레스에 전송된 이메일, 및/또는 임의의 다른 적합한 포맷과 같은, 임의의 적합한 포맷일 수 있다. 부가적으로, 몇몇 구성에서, 애플리케이션 B는 애플리케이션 A로부터 수신된 메시지를 차단함으로써 애플리케이션 A가 애플리케이션 B에 부가의 메시지를 전송하는 것을 방지할 수 있다. 유리하게는, 그 내에 포함된 커맨드(들)를 작용하기 전에 복호화된 메시지를 유효화하는 프로세스는 따라서 부가의 보안의 계층을 암호화에 제공함으로써 데이터 통신 링크의 보안을 더욱 더 향상시킨다. 예를 들어, 커맨드가 무효한 것으로 간주되면, 애플리케이션 B는 이를

무시하고 개인 및/또는 퍼스널 데이터를 위한 요청과 같은, 잠재적으로 해로운 요청은 대답하지 않을 수 있다.

[0043] 블록 128을 재차 참조하고 블록 122, 124 및 126으로부터 계속하면, 커맨드가 유효한 커맨드라면, 애플리케이션 A는 애플리케이션 B에 의해 전송된 암호화된 메시지를 수신할 수 있다. 블록 124를 참조하여 설명된 바와 같이, 메시지는 블록 126에서 애플리케이션 B에 의해 발생된 새로운 공개키를 포함한다. 블록 130에서, 애플리케이션 A는 블록 112에서 애플리케이션 A에 의해 발생된 새로운 PKI 개인키를 사용하여 암호화된 메시지를 복호화할 수 있다. 몇몇 구성에서, 애플리케이션 A는 비대칭 암호화 알고리즘을 사용하여 메시지를 복호화할 수 있다. 전술된 바와 같이, 이 방식으로, 애플리케이션 A 및 B의 공개키 및 개인키는 계속 동적으로 변경하여, 미권한부여된 애플리케이션이 사용되고 있는 변경하는 암호화 알고리즘을 계속 따라잡는 것을 어렵게 한다.

[0044] 애플리케이션 A는 블록 132로 진행할 수 있고, 복호화된 메시지 내에 포함된 커맨드가 유효한 커맨드인지를 결정할 수 있다. 예를 들어, 블록 118(전술됨)에 유사하게, 애플리케이션 A는 커맨드가 애플리케이션 A에 알려진 커맨드를 표현하는지를 결정할 수 있다. 몇몇 구성에서, 애플리케이션 A는 커맨드가 유효한 커맨드다라는 결정에 응답하여, 메시지가 인증되고 그리고/또는 손상되지 않았다고 결정할 수 있다.

[0045] 블록 132에서, 애플리케이션 A가 커맨드가 유효한 커맨드가 아니라고(132에서 "아니오") 결정하면, 애플리케이션 A는 블록 134에서 하나 이상의 사기 경보를 전송할 수 있다. 블록 120(전술된)에 유사하게, 애플리케이션 A는 애플리케이션 A에 의해 지시된(예를 들어, 애플리케이션 A의 제작자에 의해 지정된, 애플리케이션 A와 연계된 리스트 또는 데이터베이스 내에 저장된, 그리고/또는 임의의 다른 적합한 방식으로 지시된) 사용자 계정과 연계된 임의의 적합한 사용자 디바이스 및/또는 이메일 어드레스에 하나 이상의 사기 경보를 전송할 수 있다. 몇몇 구성에서, 사기 경보는 문자 메시지, 이메일, 푸시 알림, 및/또는 임의의 다른 적합한 포맷과 같은 임의의 적합한 포맷일 수 있다. 부가적으로, 몇몇 구성에서, 애플리케이션 A는 애플리케이션 B가 애플리케이션 A에 부가의 메시지를 전송하는 것을 방지할 수 있다.

[0046] 프로세스(100)는 136에서 종료할 수 있다.

[0047] 유리하게는, 개시된 방법은 소프트웨어 애플리케이션들 사이에 더 보안성 통신 링크를 제공한다. 이는 메시지가 애플리케이션으로부터 송신될 때마다 PKI 암호화키를 동적으로 변경함으로써 부분적으로 성취된다. 설명된 바와 같이, 이는 이러한 애플리케이션이 애플리케이션에 착신하는 메시지를 성공적으로 복호화하기 위해 동적으로 변경하는 개인키를 계속 따라잡아야 하기 때문에, 해킹 또는 스누핑 애플리케이션에 대해 이를 더 어렵고 에너지 집약적이게 한다. 더욱이, 더 보안성 통신 링크가 수신된 메시지를 유효화함으로써 그리고, 메시지가 무효한 경우에, 디바이스(들), 사용자(들), 및 안티바이러스, 안티해킹 및/또는 잠재적으로 사기의 액티비티의 다른 애플리케이션에 경고함으로써 또한 성취된다.

[0048] 다른 구성에서, 프로세스(100)는 애플리케이션 A가 블록 112에서 생성된 새로운 공개키로 애플리케이션 B에 암호화된 메시지를 송신한 후에 블록 114에서 종료한다. 유용하게, 애플리케이션 A의 키가 애플리케이션 B와 초기에 공유되는, 블록 104에서 생성된 키로부터 애플리케이션 B에 통신되는, 블록 112에서 생성된 키로 여전히 동적으로 변경되어 애플리케이션 B가 새로운 공개키를 사용하여 애플리케이션 A로의 리턴 메시지를 암호화할 수 있게 되기 때문에, 전체 프로세스(100)의 몇몇 장점이 여전히 성취된다.

[0049] 다른 구성에서, 블록 118 및 132(및 따라서 120 및 134)에서 수행된 유효화 중 하나 또는 모두는 수행되지 않는다.

[0050] 도 2를 참조하면, 개시된 요지의 몇몇 구성에 따른 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 하드웨어(200)의 예가 도시되어 있다. 도시되어 있는 바와 같이, 하드웨어(200)는 하나 이상의 서버(202), 통신 네트워크(206), 및 사용자 디바이스(208 및/또는 210)를 포함할 수 있다.

[0051] 서버(들)(202)는 애플리케이션(예를 들어, 모바일 디바이스 상에서 실행되는 애플리케이션, 랩탑 컴퓨터 또는 데스크탑 컴퓨터 상에서 실행되는 애플리케이션, 및/또는 임의의 다른 적합한 애플리케이션)과 연계된 정보 및/또는 데이터를 저장하기 위한 임의의 적합한 서버일 수 있다. 예를 들어, 몇몇 구성에서, 서버(들)(202)는 애플리케이션이 사용자 디바이스에 의해 다운로드되는 서버, 애플리케이션으로의 업데이트가 사용자 디바이스에 의해 다운로드되는 서버, 적합한 데이터(예를 들어, 애플리케이션의 사용자를 위한 사용자 데이터, 및/또는 임의의 다른 적합한 데이터)를 저장하고 그리고/또는 임의의 다른 적합한 기능을 수행하는 서버일 수 있다. 몇몇 구성에서, 서버(들)(202)는 생략될 수 있다.

[0052] 통신 네트워크(206)는 몇몇 구성에서 하나 이상의 유선 및/또는 무선 네트워크의 임의의 적합한 조합일 수 있다. 예를 들어, 통신 네트워크(206)는 인터넷, 모바일 데이터 네트워크, 위성 네트워크, 근거리 통신망, 광

역 통신망, 전화 네트워크, 케이블 텔레비전 네트워크, 와이파이 네트워크, WiMax 네트워크, 및/또는 임의의 다른 적합한 통신 네트워크 중 하나 이상을 포함할 수 있다.

[0053] 사용자 디바이스(208 및/또는 210)는 애플리케이션을 실행하고, 상이한 애플리케이션 및/또는 상이한 사용자 디바이스에 정보 및/또는 데이터를 전송하고, 그리고/또는 임의의 다른 적합한 기능을 수행하기 위한 임의의 적합한 사용자 디바이스일 수 있다. 몇몇 구성에서, 사용자 디바이스(208 및/또는 210)는 모바일 디바이스(예를 들어, 휴대폰, 랩탑 컴퓨터, 웨어러블 컴퓨터, 및/또는 임의의 다른 적합한 모바일 디바이스) 및/또는 비-모바일 디바이스(예를 들어, 데스크탑 컴퓨터, 스마트 텔레비전, 및/또는 임의의 다른 적합한 비-모바일 디바이스)를 포함할 수 있다. 몇몇 구성에서, 사용자 디바이스(208 및/또는 210)는 서로 로컬이거나 서로로부터 원격일 수 있다. 사용자 디바이스(208 및/또는 210)는 통신 링크(204)를 거쳐 서버(202)에 링크될 수 있는 통신 네트워크(206)에 하나 이상의 통신 링크(210)에 의해 접속될 수 있다.

[0054] 도면을 과도하게 복잡하게 하는 것을 회피하기 위해 단지 하나의 서버(202)만이 도 1에 도시되어 있지만, 임의의 적합한 수의 서버가 몇몇 구성에서 사용될 수 있다.

[0055] 서버(들)(202) 및 사용자 디바이스(208, 210)는 몇몇 구성에서 임의의 적합한 하드웨어를 사용하여 구현될 수 있다. 예를 들어, 몇몇 구성에서, 디바이스(202, 208, 210)는 임의의 적합한 범용 컴퓨터 또는 특수 용도 컴퓨터를 사용하여 구현될 수 있다. 예를 들어, 서버는 특수 용도 컴퓨터를 사용하여 구현될 수도 있다. 임의의 이러한 범용 컴퓨터 또는 특수 용도 컴퓨터는 임의의 적합한 하드웨어를 포함할 수 있다. 예를 들어, 도 3의 예시적인 하드웨어(300)에 도시되어 있는 바와 같이, 이러한 하드웨어는 하드웨어 프로세서(302), 메모리 및/또는 저장 장치(304), 입력 디바이스 제어기(306), 입력 디바이스(308), 디스플레이/오디오 드라이버(310), 디스플레이 및 오디오 출력 회로(312), 통신 인터페이스(들)(314), 안테나(316), 및 버스(318)를 포함할 수 있다.

[0056] 하드웨어 프로세서(302)는 몇몇 구성에서 범용 컴퓨터 또는 특수 용도 컴퓨터의 기능을 제어하기 위한 마이크로프로세서, 마이크로제어기, 디지털 신호 프로세서(들), 전용 로직, 및/또는 임의의 다른 적합한 회로와 같은, 임의의 적합한 하드웨어 프로세서를 포함할 수 있다.

[0057] 메모리 및/또는 저장 장치(304)는 몇몇 구성에서 프로그램, 데이터, 미디어 콘텐츠, 및/또는 임의의 다른 적합한 정보를 저장하기 위한 임의의 적합한 메모리 및/또는 저장 장치일 수 있다. 예를 들어, 메모리 및/또는 저장 장치(304)는 랜덤 액세스 메모리, 판독 전용 메모리, 플래시 메모리, 하드 디스크 저장 장치, 광학 매체, 및/또는 임의의 다른 적합한 메모리를 포함할 수 있다.

[0058] 입력 디바이스 제어기(306)는 몇몇 구성에서 디바이스로부터 입력을 제어하고 수신하기 위한 임의의 적합한 회로일 수 있다. 예를 들어, 입력 디바이스 제어기(306)는 터치 스크린으로부터, 하나 이상의 버튼으로부터, 음성 인식 회로로부터, 마이크로폰으로부터, 카메라로부터, 광학 센서로부터, 가속도계로부터, 온도 센서로부터, 근거리 센서로부터, 그리고/또는 임의의 다른 유형의 입력 디바이스로부터 입력을 수신하기 위한 회로일 수 있다.

[0059] 디스플레이/오디오 드라이버(310)는 몇몇 구성에서 하나 이상의 디스플레이/오디오 출력 회로(312)로의 출력을 제어하고 구동하기 위한 임의의 적합한 회로일 수 있다. 예를 들어, 디스플레이/오디오 드라이버(310)는 LCD 디스플레이, 스피커, LED, 또는 임의의 다른 유형의 출력 디바이스를 구동하기 위한 회로일 수 있다.

[0060] 통신 인터페이스(들)(314)는 도 2에 도시되어 있는 바와 같은 네트워크(206)와 같은, 하나 이상의 통신 네트워크와 인터페이스하기 위한 임의의 적합한 회로일 수 있다. 예를 들어, 인터페이스(들)(314)는 네트워크 인터페이스 카드 회로, 무선 통신 회로, 및/또는 임의의 다른 적합한 유형의 통신 네트워크 회로를 포함할 수 있다.

[0061] 안테나(316)는 몇몇 구성에서 통신 네트워크를 무선으로 통신하기 위한 임의의 적합한 하나 이상의 안테나일 수 있다. 몇몇 구성에서, 안테나(316)는 요구되지 않을 때 생략될 수 있다.

[0062] 버스(318)는 몇몇 구성에서 2개 이상의 구성요소(302, 304, 306, 310, 314) 사이의 통신을 위한 임의의 적합한 메커니즘일 수 있다.

[0063] 임의의 다른 적합한 구성요소가 몇몇 구성에 따라 하드웨어(300) 내에 포함될 수 있다.

[0064] 도 1의 프로세스의 전술된 블록의 적어도 몇몇은 도면에 도시되고 설명되어 있는 순서 및 시퀀스에 한정되지 않는 임의의 순서 또는 시퀀스로 실행되거나 수행될 수 있다는 것이 이해되어야 한다. 또한, 도 1의 프로세스의 상기 블록의 몇몇은 적절한 경우에 실질적으로 동시에 또는 지연 시간 및 프로세싱 시간을 감소시키기 위해 병렬로 실행되거나 수행될 수 있다. 부가적으로 또는 대안적으로, 도 1의 프로세스의 전술된 블록의 몇몇은 생략

될 수 있다.

[0065] 일 구성에서, 명령어는 메모리(304) 내에 저장되고, 명령어는 프로세스(100)의 단계의 일부 또는 모두를 수행하도록 프로세서(302)에 의해 실행 가능하다.

[0066] 다른 구성에서, 애플리케이션 A를 실행하기 위한 명령어는 제1 하드웨어(300) 상의 메모리(304) 내에 저장되고, 애플리케이션 B를 실행하기 위한 명령어는 제2 하드웨어(300) 상의 메모리(304) 내에 저장된다. 이 구성에서, 제1 및 제2 하드웨어(300)의 각각의 프로세서(302)는 애플리케이션을 실행하기 위한 명령어를 실행한다. 더욱이, 명령어는 프로세스(100)의 단계들 중 관련된 것들을 수행하기 위해 제1 및 제2 하드웨어(300)의 각각의 프로세서(302)에 의해 실행 가능한 제1 및 제2 하드웨어(300)의 각각의 메모리(304) 내에 저장될 수도 있다. 제1 및 제2 하드웨어(300)의 각각의 메모리(304) 및 프로세서(302)는 버스(318)를 거쳐 통신 가능하게 커플링된다. 더욱이, 애플리케이션 A 및 B는 제1 및 제2 하드웨어(300)의 각각의 통신 인터페이스(들)(314)를 거쳐 통신 네트워크(206)를 통해 통신할 수 있다.

[0067] 데이터는 애플리케이션 A로부터 애플리케이션 B로 직접적으로 또는 간접적으로 전송될 수 있다. 유사하게, 데이터는 애플리케이션 B로부터 애플리케이션 A로 직접적으로, 또는 간접적으로 전송될 수 있다. 일 구성에서, 데이터는 서버(202)를 거쳐 애플리케이션 중 적어도 하나로부터 애플리케이션 중 다른 하나로 전송된다. 적어도 하나의 애플리케이션에 의해 송신된 데이터는 서버(202)의 어드레스를 포함할 수도 있다. 서버(202)는 애플리케이션 중 다른 하나 상에 데이터를 포워딩할 수도 있다. 일 구성에서, 데이터는 애플리케이션과 연계된 디바이스의 구성요소를 거쳐 애플리케이션 중 적어도 하나로부터 애플리케이션 중 다른 하나로 전송된다. 예를 들어, 데이터는 적어도 하나의 애플리케이션이 실행되는 디바이스와 연계된 안테나(316)와 같은, 통신 하드웨어를 거쳐 애플리케이션 중 적어도 하나로부터 애플리케이션 중 다른 하나로 전송될 수도 있다. 데이터는 예를 들어, 안테나(316)를 거쳐, 통신 네트워크(206)를 통해 전송될 수도 있다.

[0068] 본 명세서에 개시된 프로세스는 컴퓨터 프로그램 제품에 의해 구현될 수도 있다. 컴퓨터 프로그램 제품은 전술된 다양한 프로세스 중 하나 이상의 기능을 수행하도록 컴퓨터에 명령하도록 배열된 컴퓨터 코드를 포함할 수도 있다. 이러한 방법을 수행하기 위한 컴퓨터 프로그램 제품 및/또는 코드는 컴퓨터 판독 가능 매체 상에서 컴퓨터와 같은 장치에 제공될 수도 있다. 몇몇 구현예에서, 임의의 적합한 컴퓨터 판독 가능 매체는 본 명세서에 설명된 기능 및/또는 프로세스를 수행하기 위한 명령어를 저장하기 위해 사용될 수 있다. 예를 들어, 몇몇 구현예에서, 컴퓨터 판독 가능 매체는 일시적 또는 비일시적일 수 있다. 예를 들어, 비일시적 컴퓨터 판독 가능 매체는 비일시적 형태의 자기 매체(하드 디스크, 플로피 디스크 등과 같은), 비일시적 형태의 광학 매체(광학 디스크, 디지털 비디오 디스크, 블루레이 디스크 등), 비일시적 형태의 반도체 매체[플래시 메모리, 전기 프로그램 가능 판독 전용 메모리(electrically programmable read only memory: EPROM), 전기 소거 가능 프로그램 가능 판독 전용 메모리(electrically erasable programmable read only memory: EEPROM) 등], 전송 중에 일시적이지(fleeting) 않거나 또는 어떠한 가상의 영구성(semblance of permanance)도 없는 임의의 적합한 매체, 및/또는 임의의 적합한 유형 매체(tangible media)와 같은 매체를 포함할 수 있다. 다른 예로서, 일시적 컴퓨터 판독 가능 매체는 네트워크 상에, 와이어, 전도체, 광파이버, 회로, 전송 중에 일시적이지 않거나 또는 어떠한 가상의 영구성도 없는 임의의 적합한 매체, 및/또는 임의의 적합한 유형 매체 내에 신호를 포함할 수 있다.

[0069] 컴퓨터와 같은 장치는 본 명세서에 설명된 다양한 방법에 따른 하나 이상의 프로세스를 수행하기 위해 이러한 코드에 따라 구성될 수도 있다.

[0070] 이러한 장치는 데이터 프로세싱 시스템의 형태를 취할 수도 있다. 이러한 데이터 프로세싱 시스템은 분산형 시스템일 수도 있다. 예를 들어, 이러한 데이터 프로세싱 시스템은 네트워크를 가로질러 분산될 수도 있다.

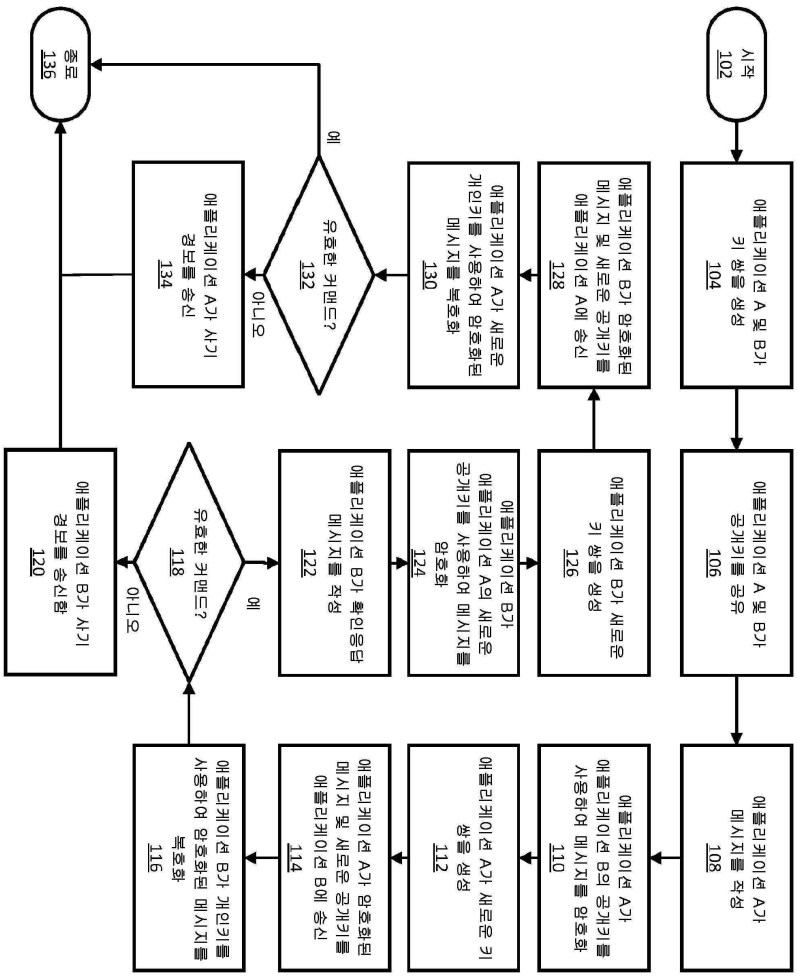
[0071] 다른 구성에서, 본 명세서에 개시된 다양한 방법 중 임의의 하나를 수행하기 위해 프로세서에 의해 실행 가능한 명령어를 포함하는 컴퓨터 판독 가능 매체가 제공된다.

[0072] 이에 따라, 암호화된 메시지를 송수신하기 위해 동적 공개키 기반 구조를 사용하기 위한 방법, 시스템, 및 매체가 제공된다.

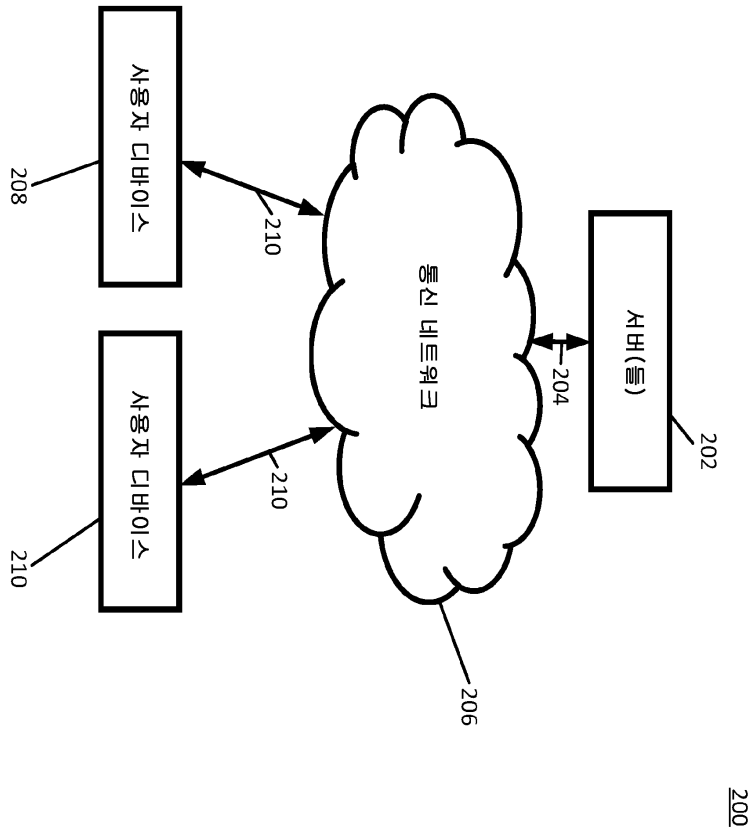
[0073] 명백한 기술적 비호환성 없이 가능한 경우에, 본 명세서에 개시된 상이한 구성 또는 양태의 특징은 선택적으로 생략되어 있는 몇몇 특징과 조합될 수도 있다.

도면

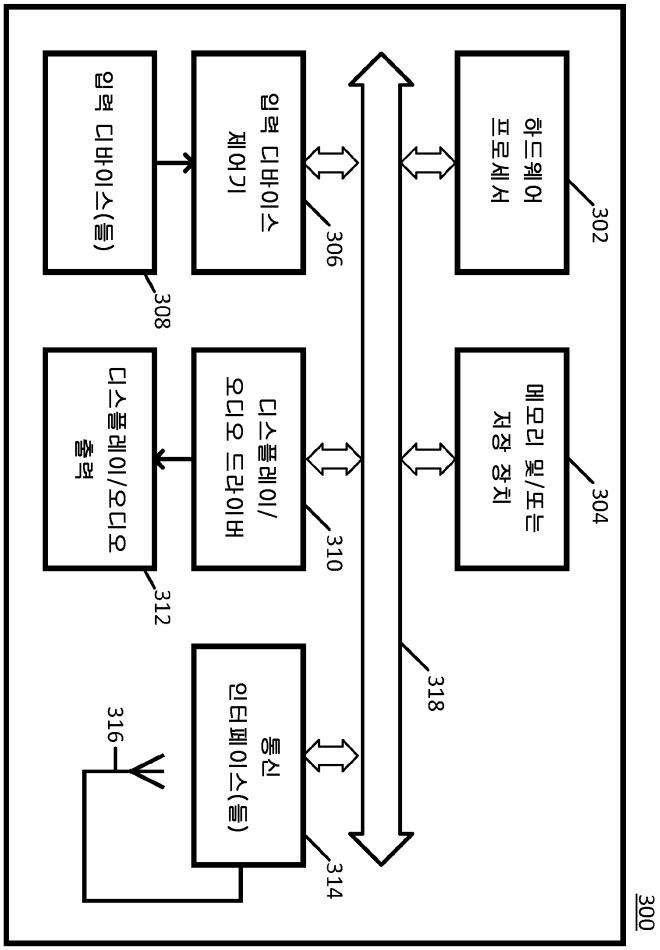
도면1


시작
102
애플리케이션 A 및 B가
키 쌍을 생성
104
애플리케이션 A 및 B가
공개키를 공유
106
애플리케이션 A가
메시지를 작성
108
애플리케이션 A가
애플리케이션 B의 공개키를
사용하여 메시지를 암호화
110
애플리케이션 A가 새로운 키
쌍을 생성
112
애플리케이션 A가 암호화된
메시지 및 새로운 공개키를
애플리케이션 B에 송신
114
애플리케이션 B가 개인키를
사용하여 암호화된 메시지를
복호화
116
유효한 커맨드?
118
예
아니오
애플리케이션 B가 확인응답
메시지를 작성
122
애플리케이션 B가
애플리케이션 A의 새로운
공개키를 사용하여 메시지를
암호화
124
애플리케이션 B가 새로운
키 쌍을 생성
126
애플리케이션 B가 암호화된
메시지 및 새로운 공개키를
애플리케이션 A에 송신
128
애플리케이션 A가 새로운
개인키를 사용하여 암호화된
메시지를 복호화
130
유효한 커맨드?
132
예
아니오
애플리케이션 A가 사기
경보를 송신
134
애플리케이션 B가 사기
경보를 송신함
120
종료
136

도면2



도면3


하드웨어 프로세서
302
메모리 및/또는 저장 장치
304
입력 디바이스 제어기
306
입력 디바이스(들)
308
디스플레이/오디오 드라이버
310
디스플레이/오디오 출력
312
통신 인터페이스(들)
314
안테나
316
버스
318
300